27. 7. 2004

PCT/JP 2004/009860

# 日 本 国 特 許 庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

| | |
|---|---|
| 出願年月日<br>Date of Application: | ２００３年１１月１７日 |
| 出願番号<br>Application Number: | 特願２００３－３８７２１２ |
| [ST. 10/C]: | [ＪＰ２００３－３８７２１２] |
| 出願人<br>Applicant(s): | 株式会社インテリジェントウェイブ |





２００４年 ７月２２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋



出証番号 出証特２００４－３０６４５９５

【書類名】　特許願
【整理番号】　P03-56
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 13/00
【発明者】
　【住所又は居所】　東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内
　【氏名】　青木　修
【発明者】
　【住所又は居所】　東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内
　【氏名】　白杉　政晴
【発明者】
　【住所又は居所】　東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内
　【氏名】　小出　研一
【発明者】
　【住所又は居所】　東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内
　【氏名】　河野　裕晃
【特許出願人】
　【識別番号】　397067853
　【氏名又は名称】　株式会社インテリジェントウェイブ
【代理人】
　【識別番号】　100117592
　【弁理士】
　【氏名又は名称】　土生　哲也
【手数料の表示】
　【予納台帳番号】　146663
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
コンピュータに不正な操作を実行させる不正データを監視するためのプログラムであって、前記コンピュータに、
前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得ステップと、
前記入出力データからユーザを識別する識別情報を特定する識別情報特定ステップと、
前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得ステップと、
前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定する不正データ判定ステップと、
前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作を停止させる第一の停止ステップと、を実行させるためのプログラムであって、
前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、
前記不正データ判定ステップにおいては、前記属性情報取得ステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること
を特徴とする不正監視プログラム。
【請求項２】
前記コンピュータに、
前記ユーザ情報格納部を参照して、前記識別情報に対応するユーザが前記コンピュータの利用権限を有しているかを判定する利用権限判定ステップと、
前記利用権限判定ステップにおいて利用権限が無いと判定された場合には、前記入出力データにより実行される操作を停止させる第二の停止ステップと、を実行させること
を特徴とする請求項１記載の不正監視プログラム。
【請求項３】
前記利用権限判定ステップを前記不正データ判定ステップより先行して実行させ、
前記利用権限判定ステップにおいて利用権限が無いと判定された場合には、前記属性情報取得ステップ、又は前記不正データ判定ステップ、又は前記第一の停止ステップの少なくとも一つのステップを実行させないこと
を特徴とする請求項２記載の不正監視プログラム。
【請求項４】
前記データ取得ステップにおいて、ネットワークから前記入出力データを取得した場合には、前記第一の停止ステップ又は前記第二の停止ステップにおいては、セッションの切断処理を実行させること
を特徴とする請求項１乃至３記載の不正監視プログラム。
【請求項５】
前記データ取得ステップにおいて、外部接続バスから前記入出力データを取得した場合には、前記第一の停止ステップ又は前記第二の停止ステップにおいては、ドライバの実行する処理を停止させること
を特徴とする請求項１乃至３記載の不正監視プログラム。
【請求項６】
前記コンピュータに、
前記入出力データにかかるログデータを、ユーザ毎のプロファイルとして格納するプロファイル格納部を参照して、前記データ取得ステップにおいて取得された入出力データが前記ユーザの日常的な操作の傾向に比して特異かを判定する特異操作判定ステップと、
前記特異操作判定ステップにおいて特異と判定された場合には、前記入出力データにより実行される操作を停止させる第三の停止ステップと、を実行させること
を特徴とする請求項１乃至５いずれかに記載の不正監視プログラム。

【請求項７】
コンピュータに不正な操作を実行させる不正データを監視するためのプログラムであって、前記コンピュータに、
前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得ステップと、
前記入出力データからユーザを識別する識別情報を特定する識別情報特定ステップと、
前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得ステップと、
前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定する不正データ判定ステップと、
前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知する通知ステップと、を実行させるためのプログラムであって、
前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、
前記不正データ判定ステップにおいては、前記属性情報取得ステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること
を特徴とする不正監視プログラム。
【請求項８】
コンピュータに不正な操作を実行させる不正データを監視するための方法であって、
前記コンピュータが、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得ステップと、
前記コンピュータが、前記入出力データからユーザを識別する識別情報を特定する識別情報特定ステップと、
前記コンピュータが、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得ステップと、
前記コンピュータが、前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定する不正データ判定ステップと、
前記コンピュータが、前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作を停止させる第一の停止ステップと、を実行させるためのプログラムであって、
前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、
前記不正データ判定ステップにおいては、前記属性情報取得ステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること
を特徴とする不正監視の方法。
【請求項９】
前記コンピュータが、前記ユーザ情報格納部を参照して、前記識別情報に対応するユーザが前記コンピュータの利用権限を有しているかを判定する利用権限判定ステップと、
前記コンピュータが、前記利用権限判定ステップにおいて利用権限が無いと判定された場合には、前記入出力データにより実行される操作を停止させる第二の停止ステップと、を有すること
を特徴とする請求項８記載の不正監視の方法。
【請求項１０】
前記利用権限判定ステップを前記不正データ判定ステップより先行して実行させ、
前記利用権限判定ステップにおいて利用権限が無いと判定された場合には、前記属性情報取得ステップ、又は前記不正データ判定ステップ、又は前記第一の停止ステップの少なくとも一つのステップを実行させないこと

を特徴とする請求項９記載の不正監視の方法。
【請求項１１】
前記コンピュータが、前記入出力データにかかるログデータを、ユーザ毎のプロファイルとして格納するプロファイル格納部を参照して、前記データ取得ステップにおいて取得された入出力データが前記ユーザの日常的な操作の傾向に比して特異かを判定する特異操作判定ステップと、
前記コンピュータが、前記特異操作判定ステップにおいて特異と判定された場合には、前記入出力データにより実行される操作を停止させる第三の停止ステップと、を有することを特徴とする請求項８乃至１０いずれかに記載の不正監視の方法。
【請求項１２】
コンピュータに不正な操作を実行させる不正データを監視するための方法であって、
前記コンピュータが、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得ステップと、
前記コンピュータが、前記入出力データからユーザを識別する識別情報を特定する識別情報特定ステップと、
前記コンピュータが、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得ステップと、
前記コンピュータが、前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定する不正データ判定ステップと、
前記コンピュータが、前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知する通知ステップと、を実行させるためのプログラムであって、
前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、
前記不正データ判定ステップにおいては、前記属性情報取得ステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること
を特徴とする不正監視の方法。
【請求項１３】
コンピュータに不正な操作を実行させる不正データを監視するためのシステムであって、
前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得手段と、
前記入出力データからユーザを識別する識別情報を特定する識別情報特定手段と、
前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納手段と、
前記ユーザ情報格納手段から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得手段と、
前記入出力データが不正データであると判定するルールを格納する判定ルール格納手段と、
前記判定ルール格納手段を参照して、前記入出力データが不正データであるかを判定する不正データ判定手段と、
前記不正データ判定手段において不正データであると判定された場合には、前記入出力データにより実行される操作を停止させる第一の停止手段と、を備えていて、
前記判定ルール格納手段には、ユーザの属性に対応する判定ルールが記憶されていて、
前記不正データ判定手段においては、前記属性情報取得手段が取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること
を特徴とする不正監視システム。
【請求項１４】

前記ユーザ情報格納手段を参照して、前記識別情報に対応するユーザが前記コンピュータの利用権限を有しているかを判定する利用権限判定手段と、
前記利用権限判定手段において利用権限が無いと判定された場合には、前記入出力データにより実行される操作を停止させる第二の停止手段と、を有すること
を特徴とする請求項１３記載の不正監視システム。
【請求項１５】
前記利用権限判定手段を前記不正データ判定手段より先行して起動し、
前記利用権限判定手段において利用権限が無いと判定された場合には、前記属性情報取得手段、又は前記不正データ判定手段、又は前記第一の停止手段の少なくとも一つを起動しないこと
を特徴とする請求項１４記載の不正監視システム。
【請求項１６】
前記入出力データにかかるログデータを、ユーザ毎のプロファイルとして格納するプロファイル格納手段と、
前記プロファイル格納手段を参照して、前記データ取得手段において取得された入出力データが前記ユーザの日常的な操作の傾向に比して特異かを判定する特異操作判定手段と、
前記特異操作判定手段において特異と判定された場合には、前記入出力データにより実行される操作を停止させる第三の停止手段と、を有すること
を特徴とする請求項１３乃至１５いずれかに記載の不正監視システム。
【請求項１７】
コンピュータに不正な操作を実行させる不正データを監視するためのシステムであって、
前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得手段と、
前記入出力データからユーザを識別する識別情報を特定する識別情報特定手段と、
前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納手段と、
前記ユーザ情報格納手段から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得手段と、
前記入出力データが不正データであると判定するルールを格納する判定ルール格納手段と、
前記判定ルール格納手段を参照して、前記入出力データが不正データであるかを判定する不正データ判定手段と、
前記不正データ判定手段において不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知する通知手段と、を備えていて、
前記判定ルール格納手段には、ユーザの属性に対応する判定ルールが記憶されていて、
前記不正データ判定手段においては、前記属性情報取得手段が取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること
を特徴とする不正監視システム。

【書類名】明細書
【発明の名称】不正監視プログラム、不正監視の方法及び不正監視システム
【技術分野】
【０００１】
本発明は、コンピュータに不正な操作を実行させる不正データを監視するための不正監視プログラム、不正監視の方法及び不正監視システムに関するものである。
【背景技術】
【０００２】
コンピュータをインターネット等のネットワークに接続して使用する場合、外部からの不正なデータの侵入を防止するとともに、コンピュータの不正操作による内部からのデータ流出や漏洩を防止することが必要になる。不正なデータの侵入を防止するためには、企業内ＬＡＮなどの内部ネットワークとインターネットの間にファイアウォールを設けて不正なデータを遮断することや、内部ネットワークや個々のコンピュータ端末にウィルスの侵入を防止するワクチンソフトを配置することが、広く行われている。ファイアウォールやワクチンソフトにおいては、キーワードや送信元のＩＰアドレスなどから不正なデータを判定するためのルールを予め定めておき、当該ルールを参照することにより不正なデータか否かを判定することが一般的である。
【０００３】
一方、不正な操作によりデータが流出することを防止するための方法については、例えばネットワークに送出されるデータに対して、アクセス権や送信元、送信する文書の種類などについて予め定められたルールを参照して、不正の恐れがあると検知されると通信を切断する技術が開示されている（例えば、特許文献１参照）。
【０００４】
【特許文献１】特開２００２－２３２４５１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
ファイアウォールやワクチンソフト、前記特許文献１記載の発明は、いずれもネットワークにおける不正なデータの侵入や漏洩を防止するためのものである。しかしながら、コンピュータを用いた不正操作はネットワークを介するものに限られず、例えば権限のない第三者が外部ネットワークには接続されていないコンピュータを不正に操作して、コンピュータ内部の情報をプリンタに出力する、ディスクに書き出す、といったネットワークを用いない方法による情報流出の危険性も存している。つまり、不正な操作を実行させるデータの監視は、ネットワークとの間だけでなく、プリンタやドライブと接続するドライバレベルにおいても行われることが好ましい。
【０００６】
また、先に説明した通り、現在の不正データの監視手法はキーワード、ＩＰアドレスやＭＡＣアドレス等を登録したルールベースを主とするものであるが、かかる方法により登録できるルールの内容には限りがある。なるべく正確な判定を行うためにはルールの数を増加させることが好ましいが、ルールの数があまりに多くなっても、判定にかかる処理が重くなるという問題が生じる。従って、多様な切り口からのルールをなるべく簡潔に登録し、かつルールの参照を効率的に行うような仕組みがあると効果的である。
【０００７】
さらに、ルールベースによる不正判定は、従来とは全く異なる方法により、登録されたルールに該当しない不正な操作を実行されると、ルールベースのみではこれを感知し難いという問題も有している。これに対しては、従来と異なるユーザの操作行動のパターンを捉えて、不正の可能性を的確に判断することができると効果的である。
【０００８】
本発明は、これらの課題に対応してなされたものであり、コンピュータに不正な操作を実行させる不正データの監視において、ネットワークのみでなく外部デバイスとの間で入

出力されるデータの監視が可能であり、かつ不正判定のための多様なルール設定と効率的なルールの適用が可能な不正監視プログラム、不正監視の方法及び不正監視システムを提供することを目的とするものである。

【課題を解決するための手段】

【０００９】

これらの課題を解決する第一の発明は、コンピュータに不正な操作を実行させる不正データを監視するためのプログラムであって、前記コンピュータに、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得ステップと、前記入出力データからユーザを識別する識別情報を特定する識別情報特定ステップと、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得ステップと、前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定する不正データ判定ステップと、前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作を停止させる第一の停止ステップと、を実行させるためのプログラムであって、前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、前記不正データ判定ステップにおいては、前記属性情報取得ステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定することを特徴とする不正監視プログラムである。

【００１０】

この発明においては、ネットワークのみでなく、コンピュータの外部接続バスを通じて入出力されるデータを監視することにより、ネットワークを経由しない不正なプリントアウトやディスクへの書き込みなどの操作を指示するデータを監視して、不正な操作を中断させることができる。また、ユーザの属性情報に応じた判定項目を加えることにより、ルールの多様化を図ることができる。

【００１１】

この発明において、コンピュータとは、ネットワークに接続され外部接続バスを備えていれば、ネットワークにおいてクライアントとして利用されるであってもよいし、サーバとして利用されるものであってもよい。ネットワークには、ＬＡＮ、ダイヤルアップなどデータの送受信が可能な全てのネットワークが含まれる。外部デバイスは、プリンタやドライブなど、外部接続バスを通してコンピュータに接続可能な全ての周辺装置が含まれる。不正データとは、外部に流出が禁じられたファイルの送信指示、権限の無いユーザによる操作など、コンピュータの不正操作にかかるデータが該当する。ユーザの属性情報には、例えばユーザの年齢、性別、所属部署、役職などが用いられる。

【００１２】

また、第一の発明は、前記コンピュータに、前記ユーザ情報格納部を参照して、前記識別情報に対応するユーザが前記コンピュータの利用権限を有しているかを判定する利用権限判定ステップと、前記利用権限判定ステップにおいて利用権限が無いと判定された場合には、前記入出力データにより実行される操作を停止させる第二の停止ステップと、を実行させることを特徴とすることもできる。さらに、前記利用権限判定ステップを前記不正データ判定ステップより先行して実行させ、前記利用権限判定ステップにおいて利用権限が無いと判定された場合には、前記属性情報取得ステップ、又は前記不正データ判定ステップ、又は前記第一の停止ステップの少なくとも一つのステップを実行させないことを特徴としてもよい。

【００１３】

第一の発明においては、ルールの一項目として用いるためにユーザの属性を予め登録するので、操作を行ったユーザがコンピュータの利用権限を有するものか否かを容易に確認することができる。ユーザの利用権限の有無をルールの判定前に行うこととすれば、最初の段階でそもそも権限を有しないユーザの操作である場合には、ルールを適用する前に操

作の停止処理を行うことにより、ルールを適用する処理を効率化することができる。

【００１４】

さらに、第一の発明は、前記データ取得ステップにおいて、ネットワークから前記入出力データを取得した場合には、前記第一の停止ステップ又は前記第二の停止ステップにおいては、セッションの切断処理を実行させることを特徴とすることもできる。又は、前記データ取得ステップにおいて、外部接続バスから前記入出力データを取得した場合には、前記第一の停止ステップ又は前記第二の停止ステップにおいては、ドライバの実行する処理を停止させることを特徴としてもよい。

【００１５】

第一の発明においては、コンピュータが実行中の処理が不正操作であると判定された場合には、即時に実行を停止させるための処理がなされる。実行中の処理がネットワークを通じたデータの送受信である場合には、実行中のセッションの切断処理を行うことにより、データの外部送信による情報漏洩等を防止することができる。実行中の処理が外部接続バスを通じた外部デバイスへの操作である場合には、ドライバの実行する処理を停止させることにより、データの出力による情報漏洩等を防止することができる。

【００１６】

さらに、第一の発明は、前記コンピュータに、前記入出力データにかかるログデータを、ユーザ毎のプロファイルとして格納するプロファイル格納部を参照して、前記データ取得ステップにおいて取得された入出力データが前記ユーザの日常的な操作の傾向に比して特異かを判定する特異操作判定ステップと、前記特異操作判定ステップにおいて特異と判定された場合には、前記入出力データにより実行される操作を停止させる第三の停止ステップと、を実行させることを特徴とすることもできる。

【００１７】

このようにユーザ毎のログデータの収集によりユーザ毎の操作の特性を把握したプロファイルを作成し、かかるプロファイルを参照してユーザが特異な操作を行ったか否かを判定することにより、ルールでは判断することのできない第三者による権限のあるユーザへのなりすまし、権限の範囲内ではあるが通常は実行しない不正の可能性のある操作などを判定することが可能になる。

【００１８】

これらの課題を解決する第二の発明は、コンピュータに不正な操作を実行させる不正データを監視するためのプログラムであって、前記コンピュータに、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得ステップと、前記入出力データからユーザを識別する識別情報を特定する識別情報特定ステップと、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得ステップと、前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定する不正データ判定ステップと、前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知する通知ステップと、を実行させるためのプログラムであって、前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、前記不正データ判定ステップにおいては、前記属性情報取得ステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定することを特徴とする不正監視プログラムである。

【００１９】

この発明においては、第一の発明は不正データと判定すると当該データにより実行される処理を停止させるのに対し、当該データにかかる処理を実行させた操作者であるユーザ、又はコンピュータや端末の管理者に対して警告を通知することにより、不正データに対処することを特徴している。

【００２０】
第一の発明及び第二の発明は、上記の不正監視プログラムの実行により行うことができる不正監視の方法として把握することもできる。また、上記の不正監視プログラムを用いた不正監視システムとして構成することもできる。
【００２１】
つまり、第一の発明は、コンピュータに不正な操作を実行させる不正データを監視するためのシステムであって、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得手段と、前記入出力データからユーザを識別する識別情報を特定する識別情報特定手段と、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納手段と、前記ユーザ情報格納手段から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得手段と、前記入出力データが不正データであると判定するルールを格納する判定ルール格納手段と、前記判定ルール格納手段を参照して、前記入出力データが不正データであるかを判定する不正データ判定手段と、前記不正データ判定手段において不正データであると判定された場合には、前記入出力データにより実行される操作を停止させる第一の停止手段と、を備えていて、前記判定ルール格納手段には、ユーザの属性に対応する判定ルールが記憶されていて、前記不正データ判定手段においては、前記属性情報取得手段が取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定することを特徴とする不正監視システムとして構成することもできる。
【００２２】
また、第一の発明は、前記ユーザ情報格納手段を参照して、前記識別情報に対応するユーザが前記コンピュータの利用権限を有しているかを判定する利用権限判定手段と、前記利用権限判定手段において利用権限が無いと判定された場合には、前記入出力データにより実行される操作を停止させる第二の停止手段と、を有することを特徴とすることもできる。前記利用権限判定手段を前記不正データ判定手段より先行して起動し、前記利用権限判定手段において利用権限が無いと判定された場合には、前記属性情報取得手段、又は前記不正データ判定手段、又は前記第一の停止手段の少なくとも一つを起動しないことを特徴としてもよい。
【００２３】
さらに、第一の発明は、前記入出力データにかかるログデータを、ユーザ毎のプロファイルとして格納するプロファイル格納手段と、前記プロファイル格納手段を参照して、前記データ取得手段において取得された入出力データが前記ユーザの日常的な操作の傾向に比して特異かを判定する特異操作判定手段と、前記特異操作判定手段において特異と判定された場合には、前記入出力データにより実行される操作を停止させる第三の停止手段と、を有することを特徴とすることもできる。
【００２４】
第二の発明は、コンピュータに不正な操作を実行させる不正データを監視するためのシステムであって、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得手段と、前記入出力データからユーザを識別する識別情報を特定する識別情報特定手段と、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納手段と、前記ユーザ情報格納手段から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得手段と、前記入出力データが不正データであると判定するルールを格納する判定ルール格納手段と、前記判定ルール格納手段を参照して、前記入出力データが不正データであるかを判定する不正データ判定手段と、前記不正データ判定手段において不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知する通知手段と、を備えていて、前記判定ルール格納手段には、ユーザの属性に対応する判定ルールが記憶されていて、前記不正データ判定手段においては、前記属性情

報取得手段が取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定することを特徴とする不正監視システムとして構成することもできる。

【発明の効果】

【００２５】

本発明により、コンピュータに不正な操作を実行させる不正データの監視において、ネットワークのみでなく外部デバイスとの間で入出力されるデータの監視が可能となり、なりすましや権限の無い者による不正なデータ出力による情報漏洩等を防止することができる。

【００２６】

また、ルールの一項目に予め登録されたユーザの属性情報を用いることにより、不正判定のための多様なルール設定を行うことが可能になる。さらに、属性情報を用いてコンピュータの操作権限の有無をルールの適用に先立って判定することにより、不正判定にかかる処理を効率化することができる。さらに、ユーザ毎の操作履歴をプロファイルとして記録することにより、ルールでは判断できない特異な操作パターンを認識し、権限のあるユーザへのなりすまし、権限の範囲内ではあるが通常は実行しない不正の可能性のある操作などを判定することも可能になる。

【発明を実施するための最良の形態】

【００２７】

本発明を実施するための最良の形態について、図面を用いて以下に詳細に説明する。尚、以下の説明は本発明の実施形態の一例であって、本発明はかかる実施形態に限定されるものではない。

【００２８】

図１、図２は、本発明にかかる不正監視システムを、それぞれネットワークの監視、外部デバイスとの接続の監視に用いる例を示す図である。図３は、本発明にかかる不正監視システムの設置位置を示す図である。図４、図５は、本発明にかかる不正監視システムの第一の構成を示すブロック図である。図６は、本発明にかかる不正監視システムのユーザデータ格納部の一例を示す図である。図７は、本発明にかかる不正監視システムの不正ルール格納部の一例を示す図である。図８は、本発明にかかる不正監視プログラムのフローを示すフローチャートである。

【００２９】

本発明にかかる不正監視システムは、ネットワークに流れる各種のデータを監視するだけでなく、プリンタなどの出力装置やディスクドライブなどの外部記憶装置をはじめとする外部デバイスと接続するための外部接続バスの監視も行うことができることを特徴としている。図３に示したとおり、本発明にかかる不正監視システムは、企業内ＬＡＮなどの内部ネットワークとインターネットのゲートウェイに設けられてネットワークを監視してもよいし、メールサーバに設けられてネットワークを通じたメールの送受信を監視してもよい。また、内部ネットワークにおけるセグメントの監視に用いてもよいし、個々のユーザ端末とネットワークとの監視、若しくは外部デバイスとの接続の監視に用いてもよい。

【００３０】

図１は、ネットワークの監視に用いる場合の一例であり、本発明にかかる不正監視システムは、不正監視サーバ１０、ユーザデータ格納部１２及び不正ルール格納部１３により構成されている。不正監視サーバ１０は、内部ネットワークとインターネットのゲートウェイに設けられて内部ネットワーク全体からの不正なデータの漏洩等を監視するものであってもよいし、内部ネットワークに設けられてセグメント内における不正なデータの漏洩等の監視に用いられるものであってもよい。

【００３１】

不正監視サーバ１０では、ネットワークを流れる全ての入出力データを取得し、ユーザデータ格納部１２からデータの入出力を行うユーザの属性にかかる情報を取得する。不正ルール格納部１３には、一般的な不正データの判定ルールに加えて、ユーザの属性に応じて不正と判定されるルールが格納されており、不正監視サーバ１０は不正ルール格納部１

３を参照して当該入出力データについて一般的な判定ルールを参照するとともに、ユーザデータ格納部１２から取得した属性に対応するルールを参照して、当該入出力データが不正か否かの判定を行う。不正と判定された入出力データに対しては、入出力が行われようとしたセッションの遮断処理を実行する。

【００３２】

図２は、外部接続バスの監視に用いる場合の一例であり、本発明にかかる不正監視システムは、処理装置２１０のＨＤＤ２１４に格納された不正監視プログラム１１、ユーザデータ格納部１２及び不正ルール格納部１３により構成されていて、これらのプログラムや格納されたデータは、監視の実行時にＨＤＤ２１４から読み出されて、処理装置２１０において演算処理される。処理装置２１０においては、ＨＤＤ２１４に格納された不正監視プログラム１１による監視を実行するために、ＲＯＭ２１３に記憶された入力制御や出力制御などのハードウェア制御のための基本的な各種プログラムを起動して、ＲＡＭ２１２を不正監視プログラム１１のワークエリアとして機能させながら、ＣＰＵ２１１が演算処理を行う。不正監視プログラム１１の演算処理においては、ＨＤＤ２１４のユーザデータ格納部１２及び不正ルール格納部１３より必要なデータが読み出されて用いられる。尚、処理装置においてプログラムを格納するＨＤＤ２１４については、フラッシュメモリなどプログラムを格納することができるその他の記憶媒体を用いるものであってもよい。

【００３３】

不正監視プログラム１１は、処理装置２１０においてドライバプログラム２２が読み出されて外部接続バス２３にプリントアウトやディスク等への書き出しの指示データが送信されると、外部接続バス２３を流れる指示データを取得し、ユーザデータ格納部１２から当該指示データにかかる操作を行ったユーザの属性にかかる情報を取得する。不正ルール格納部１３には、一般的な不正データの判定ルールに加えて、ユーザの属性に応じて不正と判定されるルールが格納されており、不正監視プログラム１１は当該指示データが不正ルール格納部１３に格納された一般的な判定ルールに該当するかを判定するとともに、ユーザデータ格納部１２から取得した属性に対応するルールに該当するかを判定する処理を実行する。不正と判定された指示データに対しては、ドライバプログラム２２により実行された処理を停止させるための処理、例えばプリントアウトの停止や外部接続バス２３に直接接続されたコンピュータとの通信の停止などの処理を実行する。

【００３４】

図１の不正監視サーバ１０、及び図２の不正監視プログラム１１における不正判定の方法について、図４及び図５を用いてさらに詳しく説明する。図４は、不正の判定ルールにユーザの属性に応じたルールを加えた判定方式を、図５はルールベースのみでなく、ユーザ毎のプロファイルから操作パターンを判定して特異な操作を不正と判定する方式を実行するための構成を示したものである。

【００３５】

図４における不正の判定は、データ取得部１４による判定の対象となるデータの取得、不正操作判定部１５によるルールベースの不正操作の判定、中断処理実行部１６による対象となる処理の中止、の順により行われる。尚、これらの各部は物理的に分離されているものではなく、各々を実行する不正監視プログラム１１の一部のプログラムとしてＨＤＤ２１４に格納されており、順次読み出されてＲＡＭ２１２をワークエリアとして機能させながら、ＣＰＵ２１１により演算処理が実行されるものであってもよい。

【００３６】

データ取得部１４は、ネットワーク又は外部接続バスを流れるデータを取得する。取得するデータには、当該データにかかる操作を実行したユーザの識別データが含まれている。識別データは、ユーザがコンピュータにログインした際のログインＩＤ等により特定される。

【００３７】

不正操作判定部１５においては、ユーザデータ格納部１２から、データ取得部１４で取得したユーザの識別データに対応するユーザの属性情報を取得する。図６は、ユーザデー

タ格納部１２に格納されたユーザの属性情報の一例であり、ユーザ毎に設けられたレコードには、ユーザＩＤと、部署や職種などの属性情報が格納されている。

【００３８】

次に、不正操作判定部１５は、不正ルール格納部１３を参照して、データ取得部１４で取得したデータが不正と判定すべきルールに該当するか否かを判定する。不正ルール格納部１３には、ユーザの属性に関わらず一般的に不正と判定すべきルールと、ユーザの属性に応じて許可されない事項を定めた属性毎のルールが格納されている。前者については、例えばキーワード、ＵＲＬ、ＩＰアドレス、ＭＡＣアドレスなどを基準に、不正の判定に一般的に用いられているルールが該当する。後者については、例えば部署や役職に応じて特定の操作について定められた操作権限などが該当する。

【００３９】

図７は不正ルール格納部１３に格納されたユーザの属性に応じて定められた判定ルールの一例であるが、ルール単位で設けられたレコードには、対象となる属性と適用されるルールが格納されており、この例では正社員以上にのみメールの送信権限を付与している。例えば、図６の例に示したインターンの看護士がメールを送信しようとすると、送信権限がないと判断されて、メールの送信処理が停止されることになる。

【００４０】

このように不正操作判定部１５において取得したデータにかかる操作が不正な操作であると判定されると、中断処理実行部１６において当該操作により実行される処理を停止させるための処理が実行される。つまり、ネットワークを通じた入出力データに対しては、入出力が行われようとしたセッションの遮断処理が実行され、外部接続バスを通じた実行処理データに対しては、プリントアウトの停止やディスクへの書き込みの停止などの処理が実行される。

【００４１】

尚、不正操作判定部１５においては、ユーザデータ格納部１２からユーザの属性情報を取得する際に、ユーザＩＤに該当するデータが存在しない場合、又はユーザＩＤが当該ユーザの退職等により無効とされている場合には、無権限者によるアクセスとして、不正ルール格納部１３による判定を行わずに不正と判定して、中断処理実行部１６による中断を実行することとしてもよい。このようにルールベースの判定の前に無権限者によるアクセスを判定すると、システムの処理負担を軽減し、速やかな判定と中断処理を実行することが可能になる。

【００４２】

図５における不正の判定は、データ取得部１４による判定の対象となるデータの取得、不正操作判定部１５によるルールベースの不正操作の判定、特異操作判定部１８によるルールベースによらないユーザ毎の操作パターンからの不正操作の判定、中断処理実行部１６による対象となる処理の中止、がそれぞれ実行される。尚、これらの各部については物理的に分離されたものではなく、各々を実行する不正監視プログラム１１の一部のプログラムとしてＨＤＤ２１４に格納されており、順次読み出されてＲＡＭ２１２をワークエリアとして機能させながら、ＣＰＵ２１１により演算処理が実行されるものであってもよいのは、図４の場合と同様である。

【００４３】

図５においても、データ取得部１４による判定の対象となるデータの取得と、不正操作判定部１５によるルールベースの不正操作の判定、中断処理実行部１６による対象となる処理の中止についての処理は、図４の場合と同様である。この構成においては、プロファイル作成部１９においてユーザ毎のプロファイルを作成し、特異操作判定部１８ではユーザ毎の操作パターンから不正操作を判定する点に特徴を備えている。

【００４４】

データ取得部１４において取得されたデータは、ルールベースによる判定を行う不正操作判定部１５とともに、ユーザ毎の操作パターンによる判定を行う特異操作判定部１８により判定が実行される。ユーザプロファイル１７には各々のユーザの過去の操作パターン

が登録されており、特異操作判定部１８では取得したデータにかかる操作とユーザプロファイル１７に登録された当該ユーザの操作パターンを対比して、特異な操作であると判定する場合には、中断処理実行部１６による中断を実行する。例えば、通常は操作を行わない時間帯に操作を行った場合、通常は実行しないタイプの操作を大量に実行した場合などは、当該ユーザによる不正行為や他人のユーザＩＤを用いたなりすましである可能性があるとして、処理が中断される。

【００４５】

尚、ユーザプロファイル１７へ登録される操作パターンは、特異操作判定部１８において判定に用いたデータと、ユーザデータ格納部１２のユーザの属性情報から作成することができる。データ取得部１４において取得したデータのログを用いることとしてもよい。プロファイルの更新は、新たなデータを取得する毎にオンライン処理として実行してもよいし、定期的なバッチ処理により行ってもよい。

【００４６】

特異操作判定部１８には、ユーザプロファイル１７に比して特異な操作パターンを判定するための、知識エンジンが設けられている。知識エンジンは通常の操作と特異な操作を判別する人工知能の機能を備えているが、人工知能の構造はベイジアン・ネットワークによるものであってもよいし、ニューラル・ネットワークによるものであってもよい。

【００４７】

尚、これまで説明した実施形態においては、不正操作と判定されるとセッションの遮断処理が実行され、外部接続バスを通じた実行処理データに対しては、プリントアウトの停止やディスクへの書き込みの停止などの処理が実行されることとして更正しているが、不正操作と判定された場合には、当該操作を実行したユーザや、コンピュータやネットワークの管理者に対して警告を通知するよう構成してもよい。

【００４８】

図８のフローチャートを用いて、本発明にかかる不正監視プログラムの基本的なフローについて説明する。まず、ネットワーク又は外部接続バスを流れる入出力データと、当該入出力データにかかる操作を実行した操作者のＩＤを取得する（Ｓ０１）。取得したＩＤについて、ユーザの属性情報を格納するユーザデータベースを参照し（Ｓ０２）、ユーザデータベースに当該ＩＤが存在しない場合には（Ｓ０３）、操作権限の無い者による操作と判断して、当該入出力データにかかる操作の中止処理を実行する（Ｓ０８）。

【００４９】

ユーザデータベースに当該ＩＤが存在する場合には（Ｓ０３）、当該ＩＤにかかる属性情報をユーザデータベースから取得する（Ｓ０４）。続いてルールデータベースを参照して（Ｓ０５）、まず取得した属性が属性毎に定められたルールに該当しないかを判定する（Ｓ０６）。該当する場合には、当該操作にかかる操作権限の無い者による操作と判断して、当該入出力データにかかる操作の中止処理を実行する（Ｓ０８）。該当しない場合には、続いて取得した入出力データが一般的なルールに該当しないかを判定する（Ｓ０７）。該当する場合には、当該操作は不正な操作であると判断して、当該入出力データにかかる操作の中止処理を実行する（Ｓ０８）。該当しない場合には、正常な操作であるとして、そのまま当該入出力データにかかる操作が実行される。

【図面の簡単な説明】

【００５０】

【図１】本発明にかかる不正監視システムを、ネットワークの監視に用いる例を示す図である。

【図２】本発明にかかる不正監視システムを、外部デバイスとの接続の監視に用いる例を示す図である。

【図３】本発明にかかる不正監視システムの設置位置を示す図である。

【図４】本発明にかかる不正監視システムの第一の構成を示すブロック図である。

【図５】本発明にかかる不正監視システムの第二の構成を示すブロック図である。

【図６】本発明にかかる不正監視システムのユーザデータ格納部の一例を示す図であ

る。

【図７】本発明にかかる不正監視システムの不正ルール格納部の一例を示す図である。

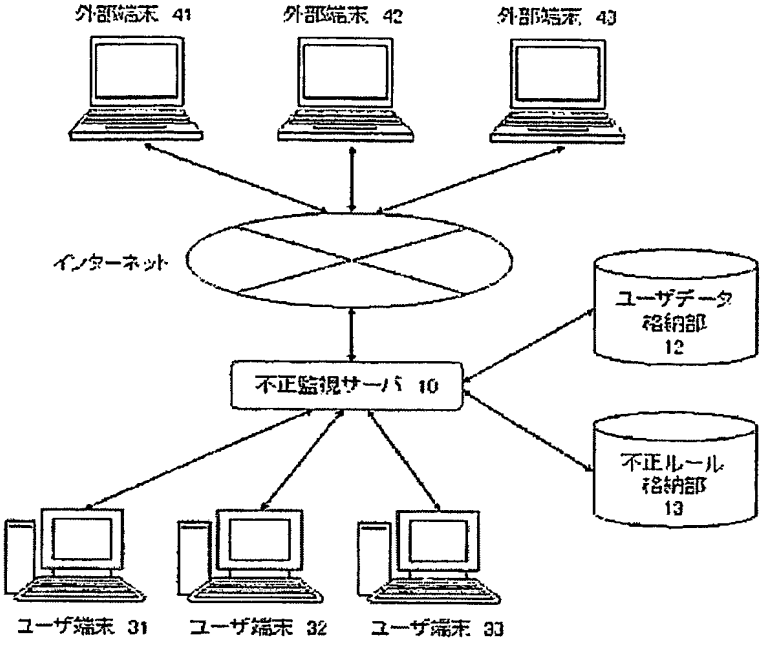
【図８】本発明にかかる不正監視プログラムのフローを示すフローチャートである。

【符号の説明】

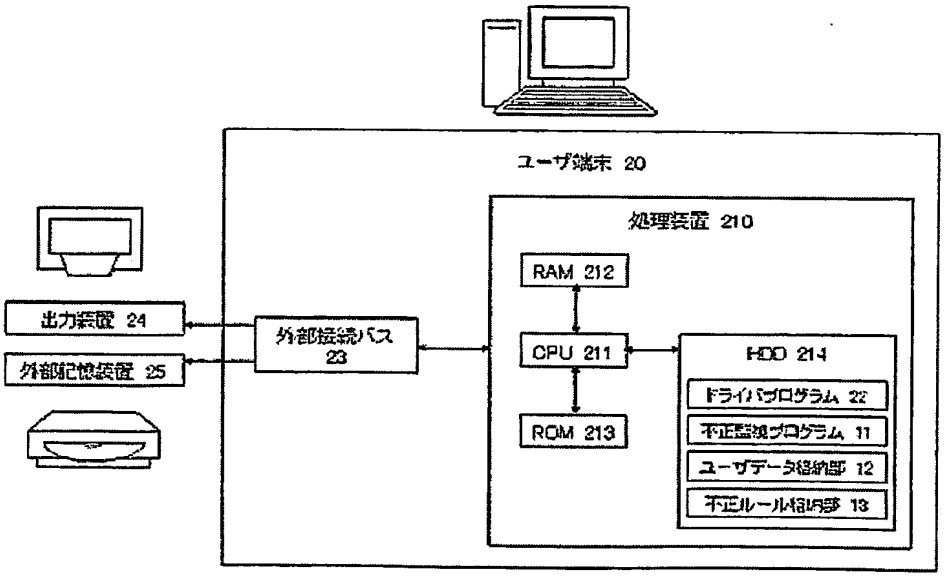
【００５１】

１０　不正監視サーバ
１１　不正監視プログラム
１２　ユーザデータ格納部
１３　不正ルール格納部
１４　データ取得部
１５　不正操作判定部
１６　中断処理実行部
１７　ユーザプロファイル
１８　特異操作判定部
１９　プロファイル作成部
２０　ユーザ端末
２１０　処理装置
２１１　ＣＰＵ
２１２　ＲＡＭ
２１３　ＲＯＭ
２１４　ＨＤＤ
２２　ドライバプログラム
２３　外部接続バス
２４　出力装置
２５　外部記憶装置
３１　ユーザ端末
３２　ユーザ端末
３３　ユーザ端末
４１　外部端末
４２　外部端末
４３　外部端末

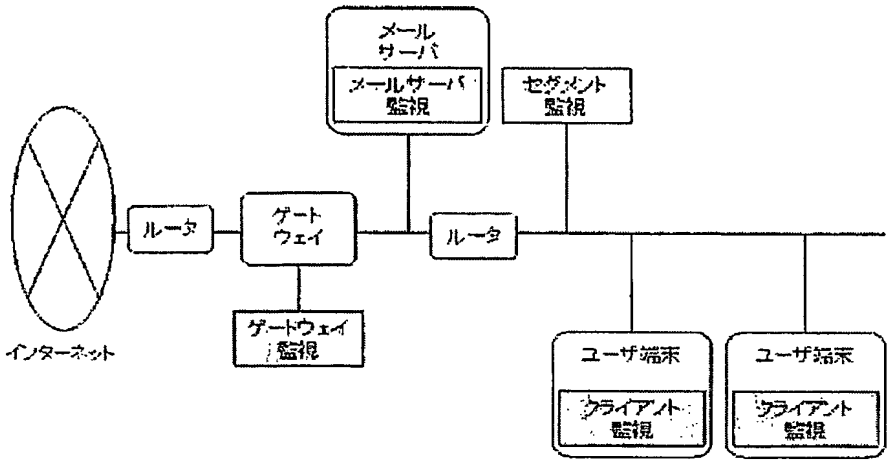
【書類名】図面
【図１】


外部端末 41
外部端末 42
外部端末 43
インターネット
ユーザデータ
格納部
12
不正監視サーバ 10
不正ルール
格納部
13
ユーザ端末 31
ユーザ端末 32
ユーザ端末 33

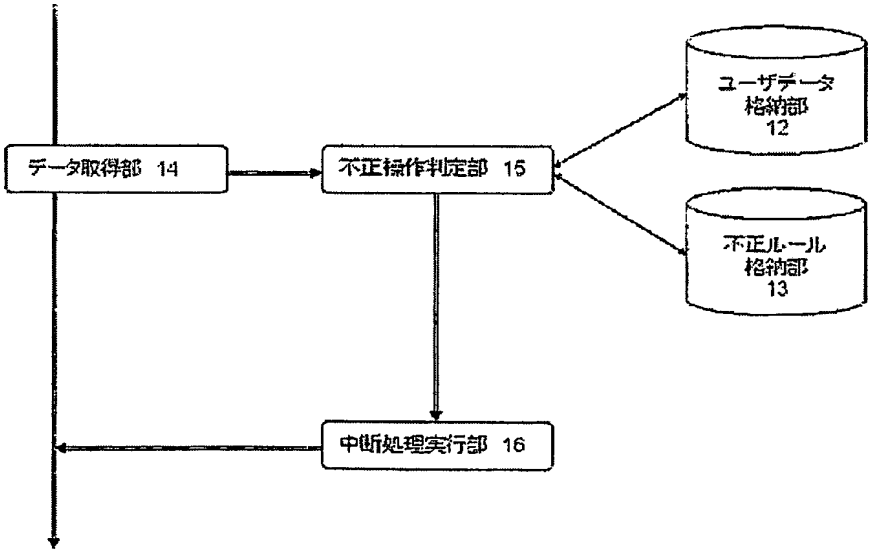
【図２】


ユーザ端末 20
処理装置 210
RAM 212
CPU 211
ROM 213
HDD 214
ドライバプログラム 22
不正監視プログラム 11
ユーザデータ格納部 12
不正ルール格納部 13
出力装置 24
外部記憶装置 25
外部接続バス
23

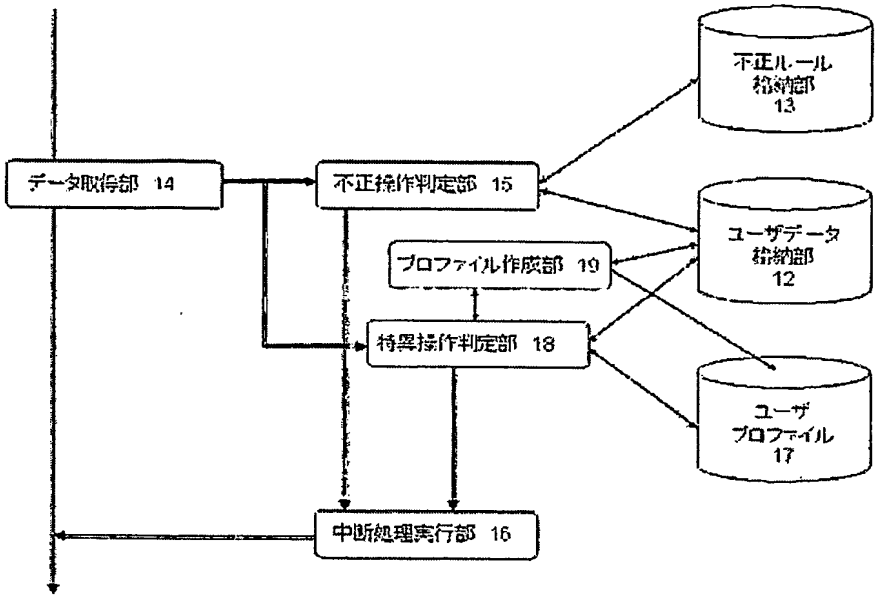
【図３】


メール
サーバ
メールサーバ
監視
セグメント
監視
ルータ
ゲート
ウェイ
ルータ
インターネット
ゲートウェイ
監視
ユーザ端末
クライアント
監視
ユーザ端末
クライアント
監視

【図４】


ユーザデータ
格納部
12
データ取得部 14
不正操作判定部 15
不正ルール
格納部
13
中断処理実行部 16

【図５】



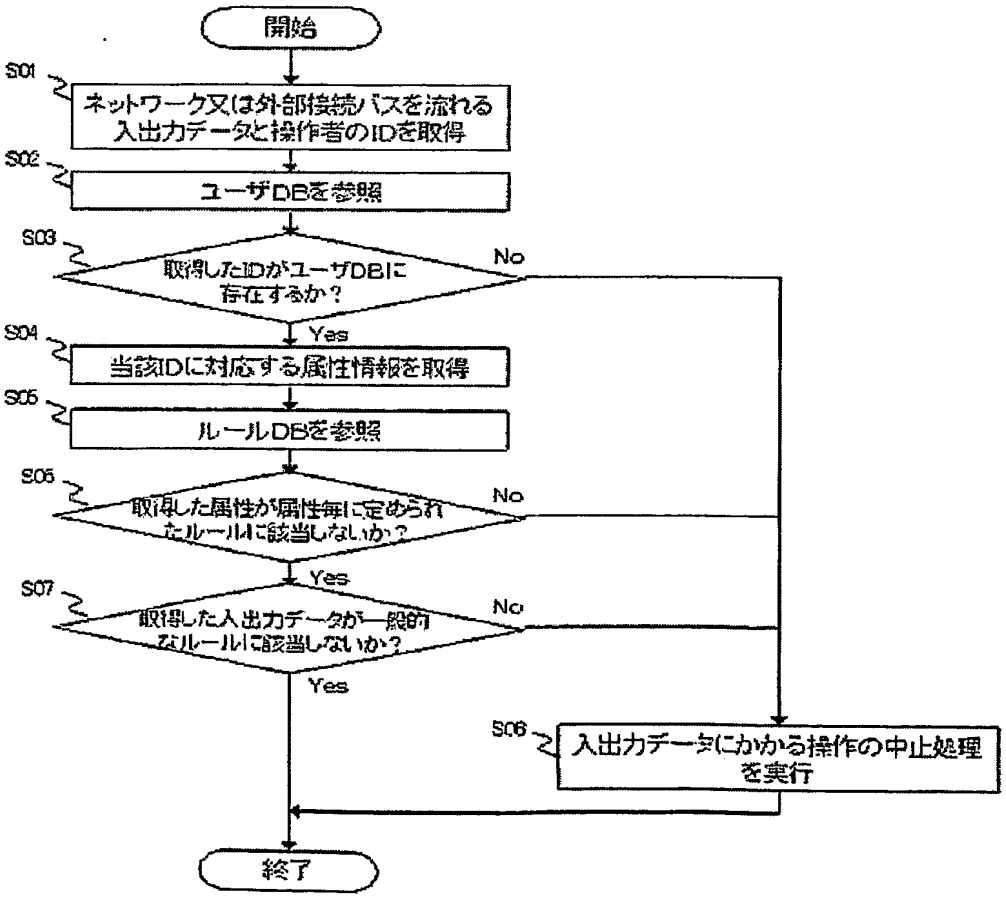

【図６】

| | |
|---|---|
| ユーザID | 0001 |
| ユーザネーム | ○○ ×× |
| 部署 | 外科 |
| 部門 | 第2 |
| 職種 | 看護士 |
| 役職 | 一般 |
| ステータス | インターン |

【図７】

| | |
|---|---|
| ルールコード | a1111 |
| 部署 | 外科 |
| 部門 | 第2 |
| 動作 | メール送信 |
| ルール | 正社員以上 |

【図８】



【書類名】要約書
【要約】
【課題】　コンピュータに不正な操作を実行させる不正データの監視において、ネットワークのみでなく外部接続デバイスとの間の入出力データの監視が可能であり、かつ不正判定のための多様なルール設定と効率的なルールの適用が可能な不正監視プログラムを提供する。
【解決手段】　データ取得部１４は、ネットワーク又は外部接続バスを流れる入出力データと操作者のＩＤを取得する。不正操作判定部１５においては、ユーザデータ格納部１２から当該ＩＤに対応するユーザの属性情報を取得して、不正ルール格納部１３に格納されたユーザの属性毎に定められたルールから当該属性情報に対応するルールを参照し、さらに不正ルール格納部１３に格納された属性に関わらず一般的に不正と判定すべきルールを参照して、不正の判定を行う。不正な操作であると判定されると、中断処理実行部１６において当該操作により実行される処理を停止させる。
【選択図】　図４

# 認定・付加情報

| | |
|---|---|
| 特許出願の番号 | 特願２００３－３８７２１２ |
| 受付番号 | ５０３０１８９８９０２ |
| 書類名 | 特許願 |
| 担当官 | 第七担当上席　　００９６ |
| 作成日 | 平成１５年１１月１８日 |

＜認定情報・付加情報＞

【提出日】　平成15年11月17日

特願２００３－３８７２１２

# 出　願　人　履　歴　情　報

識別番号　［３９７０６７８５３］

１．変更年月日　１９９７年１０月２８日
［変更理由］　新規登録
住　所　東京都江東区木場５丁目１２番８号
氏　名　株式会社インテリジェントウェイブ